Best Practice Guidelines for Establishing and Maintaining Passwords

1 CHOOSING A PASSWORD

This document outlines best practices that require consideration when initially setting up passwords (including password naming conventions), locking access to a user's account, and establishing and managing the steps for expiration of the password. The following contain general best practices and recommendations, as password requirements may differ by system.

2 SETTING UP PASSWORDS

A standard practice should be followed when creating a secure password. As systems requirements for password setting may be different and may necessitate additional requirements for setting and managing the password, this document serves only to establish best practice considerations for addressing this function.

2.1 Creating a Secure Password

The following principles should be considered for creating a secure password:

- Use a minimum of seven characters; for stronger security, create a longer password
- Your password should be easy for you to remember, but difficult for others to figure out
- If allowed by the system, intersperse punctuations marks or symbols such as %, $, *, etc.
- Mix upper- and lowercase letters together
- Never write down your password; commit it to memory
- Your password should be unique and not the same one you use for your ATM card or your email address

2.2 Things to Avoid

Avoid the following when creating a secure password:

- Use of dictionary or slang words
- Use of foreign words
- Use of simple transformations of words
- Names, double names, first name and last initial, email names
- Words made up only of uppercase or lowercase letters
- An alphabet (abcde) or keyboard (asdfg) sequence
- Words with the vowels omitted
- Phone numbers, birth dates, social security numbers
- Numbers substituted for letters (replacing the letter o with a zero (0))

3 LOCKING OF ACCOUNT

Many systems automatically lock accounts if usernames or passwords are entered incorrectly. This generally occurs after a certain number of attempted sign-ons. If this occurs, the end-user should contact the application or systems administrator or the local help desk for assistance.

4 EXPIRATION OF PASSWORD

Depending on the system design, your password may expire after a certain amount of time. Regardless of system design requirements, passwords should be changed for the following reasons:

- Your password fails to meet the criterion listed above
- You have had the same password for more than 6 months
- Someone else knows your password

- You have written down your password
- You have logged on to a system in a public place

5 SYSTEM ADMINISTRATOR MANAGEMENT

Best practices for system administrator management of passwords includes the following:

- Establish and manage a secure Log of UserID and Password
    - UserID and end-user name not linked in the log
    - Access to the log is controlled
- Set up technical controls for password expiration notification
- Set up technical controls to assure old passwords are not re-used
- Set up key identification data points/questions to assure authentic end-user is requesting system access (or re-set of password)